代数仕様言語CafeOBJによる セキュリティプロトコルの形式化

加藤 淳 (210020)

北陸先端科学技術大学院大学 情報科学研究科

2004年2月13日

キーワード: セキュリティプロトコル，Otway-Rees認証プロトコル，観測遷移機械 (OTS)，CafeOBJ.

1 はじめに

本研究の目的は，認証プロトコルの一つであるOtway-Rees Protocolを代数仕様言語CafeOBJを用いて形式的に記述し，その仕様の検証をおこなうことである．

近年，インターネットに代表される広域情報ネットワークの急速な普及および発展に伴い，ネットワークセキュリティに対する安全性の重要性が増している．ネットワーク上でメッセージを暗号化し通信者間の秘密通信機能を持つ通信プロトコルであるセキュリティプロトコルは，電子商取引や電子選挙等への適用が期待されている．

しかし，安全性が保証されているようなどんなに強固な暗号を用いてもセキュリティプロトコルに欠陥がある場合，悪意のあるユーザに欠陥を利用され秘密情報を知られてしまう可能性があり安全であるとはいえない．安全な通信を保証するセキュリティプロトコルを考案することは非常に重要なことである．一般にセキュリティプロトコルの欠陥を人間の直感による判断や，プロトコルの運用上で発見することは不具合な状態を予測するのに限界があるため非常に難しい．一方で形式手法による検証では文法・意味が数学的な厳密さで定義されており，システムの信頼性に高い効果が得られる．この形式手法による検証によりよく知られたセキュリティプロトコルの不具合が報告されたことで，その有効性が期待され，多くの手法が考案されている．

2 Otway-Rees認証プロトコル

セキュリティプロトコルの例題として，Otway-Rees Protocolを取り上げる．Otway-Rees Protocolは２つの主体が秘密の通信をおこなうために，認証局に共通鍵を発行してもらうことを目的としたプロトコルで，共通鍵暗号を利用する．Otway-Rees Protocolではノンスと呼ばれる (疑似) 乱数のような類推不可能である値を用いる．このノンスを認証局と

ある主体との共通鍵で暗号化すると，ノンスを第三者が知ることはできない．2 つの主体のための共通鍵を発行する認証局は信頼できるものと仮定する．本研究ではプロトコルに欠陥がないことを確認するため，暗号自体の信用度とは切り離して議論をおこない，暗号は絶対解読できないとする．

3 観測遷移機械

対象システムの記述には観測遷移機械 (OTS) を用いる．OTS $\mathcal{S}$ は 3 組 $\langle \mathcal{O}, \mathcal{I}, \mathcal{T} \rangle$ で定義され，各要素は観測の集合 $\mathcal{O}$，初期状態の集合 $\mathcal{I}$，条件付遷移規則の集合 $\mathcal{T}$ を表している．OTS では，対象システムの状態は観測によってのみ特定することができる．遷移規則による状態遷移は観測値の変化によって表わされる．

OTS $\mathcal{S}$ は CafeOBJ で記述する．CafeOBJ では等式を用いてシステムの振舞を記述する CafeOBJ は，記述された等式を左から右への書き換え規則として用いて，与えられた項を書き換える．この実行可能性により，記述したシステムのシミュレーションをおこなったり，システムがある性質を有することを検証することができる．

4 セキュリティプロトコルのモデル化

Otway-Rees Protocol をモデル化する際には,「プロトコルの攻撃者はどういったことをするのか」などのようにどういう仮定の下でプロトコルをモデル化するのかを定義する必要がある．

まず、使用するデータ型の定義を行う．プロトコルに登場する主体，認証局，ノンス，共通鍵，暗号文，メッセージを媒介するネットワーク等を表わすデータ型を宣言する．侵入者は主体及び認証局のデータ型の定数として定義し，主体や認証局になりすますことができるようにする．

Otway-Rees 認証プロトコルは OTS でモデル化する．メッセージの送受信により，観測可能な値がどのように変化するかを定義する．観測するものはプロトコルでそれまでに使用した 2 種類のノンス，プロトコルに関連するメッセージを媒介するネットワーク，セッション毎に生成される共通鍵の 4 つである．初期条件は，任意の初期状態を表わす定数を宣言し，観測演算の初期状態における返値を宣言する．遷移規則はプロトコルに則り Message1 から Message4 を送信する 4 種類の遷移規則，さらに，侵入者がメッセージを偽造するための 12 の遷移規則を定義する．

5 モデルの検証

プロトコルの検証は以下の手順で行う．はじめに検証したい性質を CafeOBJ で記述する．次にその性質を示すための証明譜を記述する．そして記述した証明譜を CafeOBJ 処理系で実行させ，証明譜の各部分が正しいことを検証する．検証する性質は「侵入者とは異なる主体と侵入者とは異なる別の主体のために認証局が発行した共通鍵を侵入者が不

正に入手することはない」である．

OTS $\mathcal{S}$ が安全性を有することの検証は，遷移規則の適用回数に関する帰納法を用いる．

基底段階

証明すべき述語がすべての初期状態で成り立っていることを証明する．

帰納段階

ある状態でその述語が成り立っているという仮定のもとでその状態の次の状態でも述語が成り立っていることを示す．

帰納段階では，状態空間を複数に分割する．証明譜の各段階においては項の簡約を行う．簡約結果が期待通りであれば証明が成功したことを意味する．そうでない場合は帰納法の仮定が弱いためさらに空間を分割しなければならないか，補題が必要となる．

本研究では検証する性質に対して 3 つの補題が必要であった．検証する性質及び，各補題について証明譜を記述し簡約を行った結果，すべてにおいて期待通りに `true` が得られ，プロトコルが検証したい性質，すなわち共通鍵の秘匿性を有していることを確認した．

6 まとめ

観測遷移機械を用いてセキュリティプロトコルのモデル化を行い，モデルがある性質を有していることを検証した．検証作業における場合分け・補題発見の作業は遷移規則の効力条件，および事後状態における観測値の変化に基づいてある程度までは規則的に行うことができるが，検証を行うユーザ自身が行わなければならないため，検証者の経験に依存している部分がある．

本研究では Otway-Rees 認証プロトコルの性質のうち，秘匿性 (認証局が発行した共通鍵を侵入者が入手することはできない) についての検証を行いその性質を有することを確認した．プロトコルが完全に安全性を満たすことを確認するために，加えて信頼性 (意図したメッセージが正確に送信されること) を検証しなければならない．